CLAIMS

1. An information processing device for processing encrypted data, comprising:

storage means for holding a node key unique to each of a plurality of nodes forming a hierarchical tree structure, having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices; and

encryption processing means for executing encryption processing;

said encryption processing means executing decryption processing of decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said storage means to effect calculation processing of calculating a decrypting key used in decrypting the encrypted data; said encryption processing means also effecting encrypting processing for encrypting the calculated decrypting key using a key unique to the information processing device to store the encrypted decrypting key on a recording medium or in a storage area in said information processing device.

2. The information processing device according to claim 1 wherein the key unique to said information processing device is said leaf key unique to each information processing device.

3. The information processing device according to claim 1 wherein

said key block includes a renewal key for renewing a node key stored in said storage means and said decrypting key;

said renewal node key is encrypted using a key at least including the node key or the leaf key of a lower layer;

said decrypting key is encrypted using said renewal node key; and wherein

said encryption processing means decrypts said renewal node key, using at least one of the node key or the leaf key as held by said storage means, to acquire said renewal node key; said encryption processing means calculating said decrypting key using the so acquired renewal node key.

4. The information processing device according to claim 1 wherein said encryption processing means stores said decrypting key, encrypted using the key unique to the information processing device, in association with the generation number as the renewal information for said decrypting key.

5. The information processing device according to claim 1 wherein said encryption processing means stores said decrypting key, encrypted using the key unique to the information processing device, in association with the identification information unique to said information processing device.

6. The information processing device according to claim 1 wherein said encryption processing means stores said decrypting key, encrypted using the key unique to the information processing device, in association with the identification information of encrypted data decrypted using said decrypting key.

7. The information processing device according to claim 1 wherein said decrypting key is a content key for decrypting the encrypted data.

8. The information processing device according to claim 1 wherein said decrypting key is a key allocated to said recording medium and is a media key used for decrypting encrypted data.

9. The information processing device according to claim 1 wherein said decrypting key is a key held in common with other information processing devices and is a master key used for decrypting the encrypted data.

10. An information processing device for processing encrypted data, comprising:

storage means for holding a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices; and

encryption processing means for executing encryption processing;

said encryption processing means executing decryption processing of decrypting a key block formed as key storage data that can be decryptable using at least one of said node key and the leaf key held by said storage means to effect calculation processing of calculating a decrypting key used in decrypting the encrypted data;

said encryption processing means storing the calculated decrypting key in a storage area in said information processing device in association with a generation number as the renewal information for said decrypting key.

11. An information processing device for processing encrypted data, comprising:

storage means for holding a node key unique to each of a plurality of nodes

forming a hierarchical tree structure having a plurality of such information processing devices as leaves, and a leaf key unique to each of said information processing devices; and

encryption processing means for executing encryption processing;

said encryption processing means executing decryption processing of decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said storage means to effect calculation processing of calculating a decrypting key used in decrypting the encrypted data;

said encryption processing means storing the calculated decrypting key in a storage area in said information processing device in association with the identification information used for discriminating said data decrypted using said decrypting key.

12. An information processing device for processing encrypted data, comprising:

storage means for holding a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices as leaves, and a leaf key unique to each of said information processing devices; and

decrypting processing means for executing decrypting processing;

said decrypting processing means reading in a table stored on a recording medium or in a recording area in the information processing device to retrieve whether or not a decrypting key used for decrypting the encrypted data is stored therein;

said decrypting processing means effecting decrypting processing of the

encrypted decrypting key stored on the recording medium or in the recording area in the information processing device, in case the decrypting key has been detected, to calculate the decrypting key used for decrypting the encrypted data;

said decrypting processing means effecting decrypting processing of a key block formed by decryptable key storage data, in case of failure in detecting the decrypting key, using at least one of the node key and the leaf key held by said storage means, to calculate the decrypting key used in decrypting the encrypted data.

13. The information processing device according to claim 12 wherein, if the decrypting key has not been detected, said decrypting processing means encrypts said decrypting key calculated using at least one of the node key and the leaf key held in said storage means to store the encrypted decrypting key on the recording medium or in a recording area in the information processing device.

14. The information processing device according to claim 12 wherein, if the decrypting key has been detected, said decrypting processing means decrypts the decrypting key encrypted using the key unique to each of said information processing devices.

15. An information processing method used in an information processing device, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices operating as leaves, and a leaf key unique to each of said information processing devices, comprising:

decrypting a key block formed as key storage data that can be decrypted using

at least one of said node key and the leaf key held by said information processing device;

calculating a decrypting key used in decrypting the encrypted data;

encrypting the calculated decrypting key using a key unique to the information processing device; and

storing the encrypted decrypting key on a recording medium or in a storage area in said information processing method.

16. The information processing method according to claim 15 wherein the key unique to said information processing device is said leaf key unique to each information processing device.

17. The information processing method according to claim 15 wherein said key block includes a renewal key for renewing a node key stored in said information processing device and said decrypting key;

said renewal node key is encrypted using a key at least including the node key or leaf key of a lower layer;

said decrypting key is encrypted by said renewal node key;

the decrypting processing of said key block being the processing of decrypting the renewal node key, using at least one of the node key and the leaf key as held by said information processing device, to acquire said renewal node key; and wherein

said calculating processing of said decrypting key uses the so acquired renewal node key to calculate the decrypting key.

18. The information processing method according to claim 15 wherein said decrypting key, encrypted using the key unique to the information processing device, is stored in association with a generation number as the renewal information for said decrypting key.

19. The information processing method according to claim 15 wherein said decrypting key, encrypted using the key unique to the information processing device, is stored in association with the identification information unique to said information processing device.

20. The information processing method according to claim 15 wherein said decrypting key, encrypted using the key unique to the information processing device, is stored in association with the identification information of encrypted data decrypted using said decrypting key.

21. The information processing method according to claim 15 wherein said decrypting key is a content key for decrypting the encrypted data.

22. The information processing method according to claim 15 wherein said decrypting key is a key allocated to said recording medium and is a media key used for decrypting said encrypted data.

23. The information processing method according to claim 15 wherein said decrypting key is a key held in common with other information processing devices and is a master key used for decrypting the encrypted data.

24. An information processing method used in an information processing device

adapted for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices, said method comprising:

decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said information processing device;

calculating a decrypting key used for decrypting encrypted data; and

storing the calculated decrypting key in a storage area in said information processing device in association with a generation number as the renewal information of said decrypting key.

25. An information processing method used in an information processing device adapted for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices operating as leaves, and a leaf key unique to each of said information processing devices, said method comprising:

decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said information processing device;

calculating a decrypting key used for decrypting encrypted data; and

storing the calculated decrypting key in a storage area in said information

processing device in association with the identification information for discriminating said data decrypted using said decrypting key.

26. An information processing method used in an information processing device adapted for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices, said method comprising:

reading in a table stored on a recording medium or in a storage area in an information processing device;

retrieving whether or not there is stored a decrypting key used in decrypting said encrypted data;

decrypting the encrypted decrypting key stored on said recording medium or in the recording area in said information processing device, in case the decrypting key has been detected, to calculate a decrypting key used in decrypting the encrypted data; and

decrypting, in case of failure in detecting the decrypting key, a key block formed by key storage data decryptable using at least one of the node key and the leaf key held by said information processing device, to calculate the decrypting key used in decrypting the encrypted data.

27. The information processing method according to claim 26 wherein, in case of failure in detecting the decrypting key, said decrypting key calculated using at least the node key or the leaf key held by said information processing device is encrypted using

the node key or the leaf key held on the information processing device to store the encrypted decrypting key in the recording area on said recording medium or in said information processing device.

28. The information processing method according to claim 26 wherein, if the decrypting key has been found, the encrypted decrypting key is decrypted using a key unique to each information processing device.

29. A computer program executed on an information processing device having a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices, said computer program comprising the steps of:

decrypting a key block formed as a key storage data that can be decrypted using at least one of said node key and the leaf key held by said storage means;

calculating a decrypting key used in decrypting the encrypted data;

encrypting the calculated decrypting key using a key unique to the information processing device; and

storing the encrypted decrypting key on a recording medium or in a storage area in said information processing device.

30. A computer program executed on an information processing device for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices,

operating as leaves, and a leaf key unique to each of said information processing devices, said program comprising the steps of:

decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said information processing device;

calculating a decrypting key used for decrypting encrypted data; and

storing the calculated decrypting key in a storage area in said information processing device in association with a generation number as the renewal information of said decrypting key.

31. A computer program executed on an information processing device for processing encrypted data, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices, operating as leaves, and a leaf key unique to each of said information processing devices, said computer program comprising the steps of:

decrypting a key block formed as key storage data that can be decrypted using at least one of said node key and the leaf key held by said information processing device;

calculating a decrypting key used for decrypting encrypted data; and

storing the calculated decrypting key in a storage area in said information processing device in association with the identification information for discriminating said data decrypted using said decrypting key.

32. A computer program executed on an information processing device, there being a node key unique to each of a plurality of nodes forming a hierarchical tree structure having a plurality of such information processing devices as leaves, and a leaf key unique to each of said information processing devices, said program comprising the steps of:

reading in a table stored on a recording medium or in a storage area in an information processing device;

retrieving whether or not there is stored a decrypting key used in decrypting said encrypted data;

decrypting the encrypted decrypting key stored on said recording medium or in the recording area in said information processing device, in case the decrypting key has been detected, to calculate a decrypting key used in decrypting the encrypted data; and

decrypting, in case of failure in detecting the decrypting key, a key block formed by key storage data decryptable using at least one of the node key and the leaf key held by said information processing device, to calculate the decrypting key used in decrypting the encrypted data.

33. An information recording medium in which the recorded information can be read out by an information processing device, wherein a decrypting key used for decrypting encrypted data, said decrypting key having been encrypted by a key unique to said information processing device, is recorded as a key storage table in association with the identification information for said information processing device.